



TITLE:

岩沢類数公式の一般化 (整数論)

AUTHOR(S):

片岡, 俊孝

CITATION:

片岡, 俊孝. 岩沢類数公式の一般化 (整数論). 数理解析研究所講究録
1980, 378: 47-60

ISSUE DATE:

1980-02

URL:

<http://hdl.handle.net/2433/104779>

RIGHT:

岩沢類数公式の一般化

東大 理 片岡 俊孝

§0. Introduction.

p を素数、 k を有限次代数体、 K をその無限次代数拡大とする。

もし、 K/k が \mathbb{Z}_p -拡大 (i.e. K/k は Galois 拡大であって、 $\text{Gal}(K/k)$ は、位相群として \mathbb{Z}_p と isomorphic) であるとするれば、拡大 K/k の中間体は次のように書ける。

(α) 整数 $n \geq 0$ に対して、 k 上の拡大次数が p^n である K/k の中間体 k_n が唯一存在する。

(β) $k = k_0 \subset k_1 \subset k_2 \subset \dots \subset k_n \subset \dots \subset K$ 。

(γ) $K = \bigcup_{n=0}^{\infty} k_n$ 。

このとき、 k_n の p -class group (i.e. イテ"アル類群の p -Sylow group) の位数について次のことが言える。

定理(岩沢). p, k, K, k_n は上のとおりとする。

k_n の p -class group の位数を t_n とおく。すると、非負整数 λ, μ と整数 ν が存在して

$$t_n = p^{e_n}, \quad e_n = \lambda n + \mu p^n + \nu$$

が十分大きな n に対して成り立つ。

さて、この岩沢の定理を、(a) ~ (c) をみたす有限次代数体 k 上の無限次代数拡大 K に対して拡張することを考えよう。素数 p に対して、(a) ~ (c) をみたす拡大 K/k に対して、 k_n の p -class group の位数を t_n とかく。

次の (1) 及び (2) の拡大に対しては拡張できる。

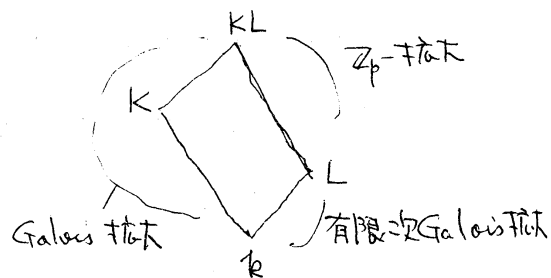
(1) 次の $(*)_p$ をみたす拡大 K/k 。ただし、 p は奇素数。

$(*)_p$ $\exists L$; k 上の有限次 Galois 拡大 s.t.

(1) KL/k : Galois 拡大,

(2) KL/L : \mathbb{Z}_p -拡大,

(3) $K \cap L = k$.



(2) $k = \mathbb{Q}$, K は k に p の p 乗根 ($\in \mathbb{R}$) をすべて添加した体 $\mathbb{Q}(\sqrt[p]{p})$ 。ただし、 p は regular prime. このときは、 $k_n = \mathbb{Q}(\sqrt[p]{p})$, $t_n = 1$ となる。

Remark 1. $(*)_p$ をみたす拡大 K/k は, (a) ~ (e) をみたす。

Remark 2. 拡大 K/k が (a) ~ (e) をみたし, しかも, k の k 上の Galois closure M に対して $\text{Gal}(M/k)$ が 1 次元 p -adic Lie group (i.e. \mathbb{Z}_p と isomorphic な open subgroup を含む群) であれば, ある整数 $n_0 \geq 0$ が存在して, K/k_{n_0} は $(*)_p$ をみたす。

以後, (1) の Case のみを扱う。この Case では, 岩沢の類数公式は次のように拡張される。

定理 1. p を奇素数とする。 k を有限次代数体, K を $(*)_p$ をみたす k 上の無限次代数拡大とする。すると, 非負整数 λ, μ と整数 ν が存在して

$$h_n = p^{e_n}, \quad e_n = \lambda n + \mu \frac{p^n - 1}{m} + \nu$$

が十分大きな n に対して成り立つ。ただし, m は k の k 上の Galois closure を M とすると, $[M:k]$ である。

Remark 1. m は, $p-1$ の約数である。

Remark 2. $m=1$ である必要十分条件は, K/k が \mathbb{Z}_p -拡大となることである。

\mathbb{Z}_p -拡大の理論については, Iwasawa [4], Lang [5] を参照。

§1. $(*)_p$ を満たす拡大の記述.

$(*)_p$ を満たす拡大 K/k に対して $(*)_p$ の (1)~(3) を満たす k 上の有限次 Galois 拡大 L の中で次のような自然なものがとれる。

命題1. p を奇素数とする。 K/k を $(*)_p$ を満たす拡大とする。すると、与えられた拡大 K/k に対して $(*)_p$ の (1)~(3) を満たす k 上の有限次 Galois 拡大 L で最小のものが存在する。そのような L について、次の (1)~(4) が言える。

- (1) L は k の m 次 cyclic extension,
- (2) KL は k の k 上の Galois closure,
- (3) $\text{Gal}(KL/k)$ は、 $\text{Gal}(KL/k)$ と normal subgroup $\text{Gal}(KL/L)$ との semi-direct product である。
- (4) Homomorphism $\varphi: \text{Gal}(KL/k) \longrightarrow \text{Aut}(\text{Gal}(KL/L))$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ \sigma & \longmapsto & (x \mapsto \sigma^{-1} x \sigma) \end{array}$$

は injective である。

さて、 $(*)_p$ を満たす拡大 K/k (特に、 $m \neq 1$ であるもの) がどの程度存在するか考えてみよう。

命題2. p を奇素数とする。 k を有限次代数体とする。

すると、次の集合間の bijective な対応が存在する。

$$\{K: K/k \text{ は } (*)_p \text{ をみたす}\} / \sim \longleftrightarrow \{(L, M) \mid (**)\}.$$

こゝに、 $(*)_p$ をみたす K に対応する (L, M) は、 $L = (*)_p$ の (1)~(3) をみたす k 上の最小の Galois 拡大、 $M = K$ の k 上の Galois closure である。逆に、 $(**)$ をみたす (L, M) に対しては、 $K = M^H$ (H は $\text{Gal}(M/k) = H \rtimes \text{Gal}(M/L)$ となる $\text{Gal}(M/k)$ の部分群) を対応させる。

ただし、“ \sim ” は k 上の共役であるという relation をあらわす。 $(**)$ は、 (L, M) に関する次のような条件 (1)~(4) のことである。

- (1) M は、 k 上の Galois 拡大、
- (2) L は、 M/k の中間体で、 M/L は \mathbb{Q}_p -拡大、
- (3) L/k は、cyclic of degree dividing $p-1$,
- (4) homomorphism $\text{Gal}(L/k) \longrightarrow \text{Aut}(\text{Gal}(M/L))$

$$\begin{array}{ccc} \downarrow & & \downarrow \\ \sigma & \longmapsto & (\alpha \mapsto \alpha^\sigma) \end{array}$$

は、injective である。ただし α^σ は $\hat{\sigma}$ を σ の M の auto. の拡張とすれば、 $\hat{\sigma}^{-1} \alpha \hat{\sigma}$ である。

$k = \mathbb{Q}$ のときは、命題 2 の対応にあらわれる L は、次のようなものである。

命題3. p を奇素数とする。 $k = \mathbb{Q}$ とする。有限次代数体 L に対して次は同値である。

- (1) (L, M) が命題2の $(*)$ をみたすような M が存在する。
- (2) $L = \mathbb{Q}$ 、あるいは、 L は \mathbb{Q} 上の imaginary cyclic extension of degree dividing $p-1$ 。

Remark. (2) \Rightarrow (1) は類体論。 (1) \Rightarrow (2) をいふには、絶対アーベル体では、Leopoldt conjecture が成立する (A. Brumer [2]) ことをつかう。

以後、 p は奇素数であるとし、 $(*)_p$ をみたす有限次代数体 k 、及び k 上の無限次代数拡大 K を固定する。 K/k に対応する (L, M) は unique に定まるから、 L, M はそのようなものをあらわすものとする。

$m = [M:k] = [L:k]$, $H = \text{Gal}(M/k)$, $\Gamma = \text{Gal}(M/L)$, $G = \text{Gal}(M/k)$ とおく。すると命題1より

$$\begin{cases} H: m\text{-cyclic}, \\ \Gamma \simeq \mathbb{Z}_p, \\ G = H \rtimes \Gamma \text{ (H と } \Gamma \text{ の semi-direct product)}. \end{cases}$$

$X(H) = \text{Hom}(H, \mathbb{Z}_p^\times)$ とおく。 $\chi \in X(H)$ に対応する idempotent を e_χ とかく。すなわち、

$$e_\chi = \frac{1}{m} \sum_{t \in H} \chi(t^{-1}) t \in \mathbb{Z}_p[H].$$

$\eta \in X(H)$ を、 $h^{-1}xh = x^{\eta(h)}$, $x \in \Gamma$, $h \in H$ で定める。すると
命題 1 の (4) より、 $X(H) = \langle \eta \rangle$ である。

§ 2. K/k と KL/L .

定理 1 の λ, μ は、 K/k のみで定まるから、それでは、
 K/k の λ -invariant, μ -invariant と呼ぶ、 $\lambda(K/k), \mu(K/k)$
とかく。これは K/k が \mathbb{Z}_p -拡大のときは、通常の設定と一致
する。 K/k と KL/L の λ -invariants と μ -invariants 間に次の
関係がある。

定理 2. (1) $\mu(KL/L) = \mu(K/k)$,
(2) $\lambda(KL/L) = m \lambda(K/k) - (m-1) + \sum_{\alpha=0}^{m-2} (m-1-\alpha) (d_{\eta^\alpha}^{(3)} - d_{\eta^{\alpha+1}}^{(3)})$.

ただし、 $\chi \in X(H)$ に対して、 $d_\chi^{(2)}, d_\chi^{(3)}$ は次のように定める。

$$d_\chi^{(2)} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \varprojlim_n (E_L / N_L k_n / L(E_L k_n))^{\otimes \chi},$$

$$d_\chi^{(3)} = \dim_{\mathbb{Q}_p} \mathbb{Q}_p \otimes_{\mathbb{Z}_p} \text{Hom}_{\mathbb{Z}_p} (H^1(\Gamma, E_{kL})^{\otimes \chi}, \mathbb{Q}_p / \mathbb{Z}_p).$$

ここに、 E_* は、 $*$ の単数群をあらわす。 $H^1(\Gamma, E_{kL})$ は、
Galois cohomology であり、自然に $\mathbb{Z}_p[H]$ -module とみな
せる。

Remark 1. 次のことに注意する。

$$H^1(\Gamma, E_{kL}) = \varinjlim_n H^1(\Gamma / \Gamma^{p^n}, E_{k_n L}),$$

$$H^1(\Gamma / \Gamma^{p^n}, E_{k_n L})^{\otimes \chi} \simeq (E_{k_n L} / E_{k_n L}^{1-\sigma})^{\otimes \chi \eta}, \quad \eta \gg 0, \quad \chi \in X(H).$$

ただし、 $\langle \sigma \rangle = \Gamma$, $E_{KL}/L = \{x \in E_{KL} \mid N_{KL/L}(x) = 1\}$ である。
 このことより、 $d_x^{(3)} - d_x^{(2)}\eta$ は、Herbrand quotient を $\mathbb{Z}_p[H]$
 の作用により細分したものと考えることができる。

Remark 2. $m=2$ のときの $\lambda(KL/L) \pmod{2}$ についての議論が、Gillard [3] にある。

§ 3. Iwasawa algebra $\mathbb{Z}_p[[G]]$.

\mathcal{O} , Λ は、それぞれ G , Γ の \mathbb{Z}_p 上の Iwasawa algebra $\mathbb{Z}_p[[G]]$, $\mathbb{Z}_p[[\Gamma]]$ とする。 R は \mathcal{O} の center とする。 \mathcal{O} は、 profinite group N に対して、 \mathbb{Z}_p 上の Iwasawa algebra $\mathbb{Z}_p[[N]]$ とは、
 $\varprojlim \mathbb{Z}_p[N/N']$ のことである。 ただし、 N' は N の open normal subgroup をわたる。 \mathcal{O} の構造は、 m , η のみによって定まることに注意する。 Λ は \mathcal{O} の subring とみなせよ。 G の元は自然に \mathcal{O} の元と思える。 \mathcal{O} , Λ , R について次のことが言える。

命題 4. (1) $R = \Lambda^H = \{\lambda \in \Lambda \mid h^{-1}\lambda h = \lambda, \forall h \in H\}$,

(2) $Y = \frac{1}{m} \sum_{x \in H} \eta(x^{-1}) (\sigma - 1)^x$ とおく。 ただし、 σ は Γ の topological generator。 すると、 $h \in H$ に対して、

$$Y^h (= h^{-1} Y h) = \eta(h) Y.$$

(3) $\Lambda = \mathbb{Z}_p[[Y]]$, $R = \mathbb{Z}_p[[Y^m]]$.

(4) \mathcal{O} は twisted group ring $\Lambda \circ H$ とみなせる。

$\chi \in X(H)$ に対して、 e_χ によつて生成される \mathcal{O} の right ideal $\in \Lambda_\chi$ とかく。これは、projective \mathcal{O} -module である。
 H の単位指標 ($\in X(H)$) を 1_H とかく。有限生成 \mathcal{O} -module N_1, N_2 に対して、 N_1 から N_2 への \mathcal{O} -homomorphism φ での Kernel も Cokernel も有限となるものが存在すれば、 N_1 は N_2 と pseudo isomorphic であり、 φ は pseudo-isomorphism と呼ぶ。有限生成 right \mathcal{O} -module は、modulo pseudo-iso. どのように決定できる。

定理 3. 有限生成 right \mathcal{O} -module は、次の modules たちの直和と pseudo-isomorphic である。

- (1) Λ_χ , $\chi \in X(H)$,
- (2) $\Lambda_{1_H} / \Lambda_{1_H} \mathfrak{f}^n$, \mathfrak{f} は (Y^n) とことなる R の height 1 の素イデアル、 n は自然数,
- (3) $\Lambda_\chi / \Lambda_\chi Y^n$, $\chi \in X(H)$, n は自然数。

このような分解は unique である。

Remark. $m=1$ のときは、すでに得られてゐる。(c.f., Bourbaki [1], Iwasawa [4], Serre [7]).

この定理は、定理2の証明に必要である。とくに、定理2 (1) は、直ちに成る。Ordersの一般論については、I. Reiner [6] を参照。

§4. 定理1の証明について。

有限次代数体 N に対して、 C_N でその p -class group をあらわす。さらに一般の代数体 N に対しても $\varprojlim C_{N'} \subseteq C_N$ とかく。ただし、 N' は N の有限次部分体をわたる。定理1は、次の順序で証明する。

i) C_K には、自然に R -module の structure がはいる、 R -module として有限生成かつ torsion である。

ii) index 有限な R -submodule C と十分大きな整数 n に対して定められた R の元よりなる列 $\{d_n\}_{n \geq 0}$ が存在して

$$(***) \quad C_{d_n} \simeq C_K / C^{d_n}$$

が、十分大きな整数 n に対して成立する。

iii) $\# C / C^{d_n}$ の計算。

このことをもう少し詳しくおしくみてみよう。

i) について： 自然な同型 $C_K \simeq C_{K, \mathbb{Z}}^{e_{1n}}$ より、 C_K に R -module の構造がはいる。 C_K が R -module として、有限生成

かつ Torsion であるのは、 C_{KL} が Λ -module としてそうだからである。

ii) について: $n_0 \in \mathbb{N}$ 、すなわち $k_{n_0}L$ の素イデアルについて、
 それが拡大 $KL/k_{n_0}L$ で分岐するならば完全分岐となるような
 非負整数とする。自然な surjective homomorphism $C_K \rightarrow C_{k_{n_0}}$
 の kernel を C とおく。次に $\ell_n \in \mathbb{N}$ 整数 $n \geq n_0$ に対して定めよう。
 まず、 $f \in \Lambda$ に対して、 $\tilde{f} \in R$ を

$$\tilde{f} = \frac{1}{m} \text{Tr}_{\Lambda/R}(f) = \frac{1}{m} \sum_{x \in H} f^x$$

で定める。Iwasawa [4] によらうて、整数 $0 \leq \alpha \leq \beta$ に対して、
 Λ の元 $v_{\alpha, \beta} \in \Lambda$ を $v_{\alpha, \beta} = (\sigma^{p^\beta} - 1) / (\sigma^{p^\alpha} - 1)$ とおく。ただし、
 σ は T の topological generator である。整数 $n \geq n_0$ に対して、
 $\ell_n = \widehat{v}_{n_0, n}$ とおく。すると、整数 $n \geq n_0$ に対して (***) が成
 り立つ。このことを示すためには、次の命題が key になる。

命題 5. 整数 $0 \leq \alpha \leq \beta$ に対して、 $u \in \Lambda^\times$ が存在して、
 $v_{\alpha, \beta} = u \tilde{v}_{\alpha, \beta}$ が成り立つ。

iii) について: 一般に有限生成 torsion R -module に対して次の
 ことが言える。

定理 4. V は有限生成 torsion R -module とする。非負整

数 n_0 に対して、すべての整数 $n \geq n_0$ が $\#V/V\hat{\mathcal{U}}_{n_0,n} < +\infty$ をみたすならば、十分大きな整数 n に対して

$$\#V/V\hat{\mathcal{U}}_{n_0,n} = p^{e_n}, \quad e_n = \lambda n + \mu \cdot \frac{p^n - 1}{p - 1} + \nu$$

が成り立つ。ただし、 λ, μ, ν は n に依存しない整数で、 λ, μ は非負である。

Remark 1. n_0 を十分大きくとれば $\#V/V\hat{\mathcal{U}}_{n_0,n} < +\infty$ はみたされる。

Remark 2. V を R -module として

$$\sum_i \oplus R/Rp^{k_i} \oplus \sum_j \oplus R/Rf_j$$

と pseudo-isomorphic であるとする。ただし、 k_i は自然数、 f_j は Υ^m に関する distinguished polynomial である。すると、定理の λ, μ は、それぞれ $\sum_i k_i, \sum_j \deg_{\Upsilon^m} f_j$ である。

Remark 3. $m=1$ のときはすでに証明されている。(c.f. Iwasawa [4], Lang [5], Serre [7]).

$p=2$ のときについて簡単に述べる。このときも命題 1 へと同様のことが言える。ただし m は 1 または 2 である。 $m=1$ ならば、拡大 $\mathbb{Q}_2/\mathbb{Q}_2$ は \mathbb{Z}_2 -拡大となるから、 $m=2$ のときのみが問題である。 \mathbb{C}, Λ, R も同様に定義できる。このとき上の i) は成立する。ii) の (***) のような記述を与えうるか否かは不明です。もし、(***) のような記述が与えられれば、

iii) はそれほど困難ではないように思われます。

Introduction で述べた (2) の型の拡大について、次のことに注意する。(2) の拡大で、 p が "irregular prime" のときも、(***) 型の記述を支えることが出来る。ただし作用している環は、 \mathbb{Z}_p 上の 2 次元の p -adic Lie group の Iwasawa algebra である。もし $L = K$ のような algebra L の module について、適当な制限のもとに、定理 3 のような modulo pseudo-isomorphism での分類ができれば、この Case にも拡張できるように思われる。

文献

- [1] N. Bourbaki, Algèbre commutative Chapitre 7, Hermann, Paris, 1965.
- [2] A. Brummer, On the units of algebraic number fields, Mathematika, 14, 1967, 121-124.
- [3] R. Gillard, Remarques sur certaines extensions proliédrales de corps de nombres, C.R. Acad. Sc. Paris, 282 (5 janvier 1976) Série A, 13-15.
- [4] K. Iwasawa, On the \mathbb{Z}_l -extensions of algebraic number fields, Ann. of Math., 98 no. 2, 1973, 246-326.
- [5] S. Lang, Cyclotomic fields, Springer, New York, 1978.
- [6] I. Reiner, Maximal orders, Academic press, London,

1975.

[7] J. P. Serre, Classes des corps cyclotomiques, Séminaire Bourbaki, Exposé 1974 (1958-1959).